UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:	)	
	)	
INFORMATION ASSOCIATED WITH	)	Magistrate No. 16-0385M
FACEBOOK USER ID **100000421615731** and	)	**[UNDER SEAL]**
100009052827992 THAT IS STORED AT PREMISES	)	
OWNED, CONTROLLED, OR OPERATED BY	)	
FACEBOOK		

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Molly Rock, being duly sworn, do hereby depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain Facebook accounts that are stored at premises owned, maintained, controlled, or operated by Facebook, a social networking company headquartered in Palo Alto, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer operating the web sites.

2. I am a Special Agent with the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the HSI Pittsburgh, Pennsylvania office. I have been employed in this position since August, 2010. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251(a), 2252(a)(2), and 2252(a)(4)(B). I have had the opportunity to observe

and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography offenses.

3. The facts in this affidavit come from my personal observations, my training and experience, information obtained from other law enforcement officers and witnesses, and the review of documents and records. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251(a), which makes it a crime to employ, use, persuade, induce, incite, or coerce a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct; 18 U.S.C. § 2252(a)(2), which make it a crime to receive and distribute child pornography in interstate commerce by computer; and violations of 18 U.S.C. §§ 2252(a)(4)(B), which make it a crime to possess or access with intent to view child pornography, have been committed by **Randolph "Randy" GUM**. There is also probable cause to search the information described in Attachment A for evidence, fruits and instrumentalities of the violations of Title 18, United States Code, Sections 2251(a), 2252(a)(2) and 2252(a)(4)(B), as described in Attachment B.

DEFINITIONS

5. The following definitions apply to this Affidavit:

6. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

7. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

8. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

9. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

10. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

11. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

12. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "email address," an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long term storage of electronic communications and many other types of

electronic data and files. Typically, email that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that email to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage," see 18 U.S.C. § 2510(17), and the provider of such a service is an "electronic communications service."

13. An "electronic communications service," as defined by statute, is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a "remote computing service." 18 U.S.C. § 2711(2).

14. "Domain names" are common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top-level domains, are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov

identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

15. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

BACKGROUND REGARDING CHILD PORNOGRAPHY AND COMPUTERS

16. Based on your Affiant's training, experience, and knowledge, your Affiant knows the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers and mobile devices (e.g., smartphones, tablets) has added to the methods used by child pornography collectors to interact with and

sexually exploit children. Computers and mobile devices serve four functions in connection with child pornography; production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs directly from a camera or mobile device to a computer storage system. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem, or via mobile devices. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer and Internet-capable mobile devices are preferred methods of distribution and receipt of child pornographic materials.

d. The advent of webcams has enabled child pornographers to broadcast live transmissions of sexual abuse of minors by connecting the webcam to the Internet. A webcam is a video camera that attaches to a computer or that is built into a laptop or desktop screen. The software included with webcams also permits an individual to capture and save live transmissions to the computer or peripheral storage devices. A webcam can be used in conjunction with an instant messaging service which permits real-time, direct, text-based communication between two or more people while permitting the individuals to view each other real-time via the webcam. However, a webcam is not required in order to receive live transmissions of activity that is taking place in front of another user's webcam.

e. The ability of a computer or mobile device to store images in digital form makes these devices an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text, and CDs, DVDs, and flash drives can store hundreds of images and thousands of pages of text. The size of the electronic storage media (commonly referred to as the hard drive or thumb drive) used in home computers has grown tremendously within the last several years. Electronic storage devices with the capacity of 750 gigabytes are common, and electronic storage devices in excess of one terabyte (1,000 gigabytes) are now available for sale for low cost. These drives can store thousands of images at very high resolution. It is possible to use digital cameras and "video" cameras (designed primarily to record moving images), including those contained in mobile devices, to upload images to the Internet. Only through careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail generated by this activity.

f. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

g. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography in various formats, including services offered by Internet Portals such as Microsoft Live, Yahoo!, Google, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or electronic device such as a phone, tablet, or other device with access to the Internet. Even in cases where online storage is used, however,

evidence of child pornography can be found on the user's computer and/or mobile devices, in most cases.

h. As is the case with most digital technology, communications by way of computer and mobile device can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files, cache, or ISP client software, among others). In addition to electronic communications, a computer or mobile device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. For example, computers often indefinitely retain archived conversations from instant messaging programs as well as messaging logs and files shared over instant messaging.

BACKGROUND OF THE INVESTIGATION & PROBABLE CAUSE

17. In May 2014, special agents from HSI Los Angeles executed a federal search warrant authorizing the search of a target's residence for violations relating to the distribution, receipt, and possession of child pornography. During the execution of the search warrant, the target of the investigation was interviewed and consented to law enforcement taking over the target's online presence, which included several different email accounts that the target used to trade child pornography.

18. HSI Riverside Special Agent (SA) Jonathan Ruiz took control of the aforementioned target's email accounts and periodically logged into these accounts, noting that

the accounts continued to receive individual and group emails containing child pornography. On or about August 7, 2015, SA Ruiz logged into one of the accounts and found that the user of the email account talentedtongue19@yahoo.com had recently sent two group emails, each containing an attached child pornography video. The emails from talentedtongue19@yahoo.com were sent to the target account, as well as approximately 90 other email recipients.

19. On August 27, 2015, SA Ruiz executed a federal search warrant on Yahoo! for the user account talentedtongue19@yahoo.com to search for evidence of the distribution, receipt, and possession of child pornography. During October 2015, Yahoo! provided SA Ruiz with information responsive to the aforementioned search warrant. SA Ruiz reviewed the information provided by Yahoo! and noted that the talentedtongue19@yahoo.com account contained numerous emails, both sent and received, that included attached images and/or videos depicting the sexual exploitation of minors, as well as discussions of the sexual abuse of children. In addition, SA Ruiz found emails sent by talentedtongue19@yahoo.com that contained hyperlinks to downloadable files, as well as solicitations to others offering to trade child pornography.

20. SA Ruiz subsequently obtained the hash values of the images and videos contained in the talentedtongue19@yahoo.com account and submitted the information to the National Center for Missing and Exploited Children (NCMEC) for identification of known victims. NCMEC reported that at least three (3) video files sent by talentedtongue19@yahoo.com and at least one (1) video file received by talentedtongue19@yahoo.com depicted an identified child victim.

21. Additionally, SA Ruiz conducted a Google.com search for talentedtongue19 and discovered a publically accessible link to a foreign-based image hosting website (hereinafter "Website A"). Website A is known to law enforcement to frequently contain images of child pornography. SA Ruiz noted the talentedtongue19 account on Website A was active and publically accessible. The profile page showed that it was registered on January 27, 2014, and that the account is registered to talentedtongue19@yahoo.com. Website A allows the user to advertise a website or "homepage" on their profile. On talentedtongue19's Website A profile page, the email address "talentedtongue14@yahoo.com" was advertised instead. Talentedtongue19's Website A profile page contained the following user-inputted information: "Please trade with me! Ill most likely send back if you send a good sample pic:)."

22. The aforementioned talentedtongue19 Website A profile page contained one photo album titled "cute." The photo album was publicly available and was not password protected. On or about August 7, 2015, SA Ruiz accessed the photo album and found it to contain 12 images. Five of the images depicted the same young male child, appearing to be under the age of 12 years old. The images were not sexual in nature. In addition, SA Ruiz noted a second Website A account for "tongueboy" that was associated with the Website A talentedtongue19 account. SA Ruiz accessed the publicly available profile page for the Website A tongueboy account, noting the account was registered on December 5, 2014. The email account associated with tongueboy was made private and displayed the message, "hidden, contact via comments." The tongueboy profile contained one image album titled "cute" and contained the following user-inputted information: "I been locked out other account but still using this email talentedtongue14@yahoo.com." SA Ruiz accessed the publically available image album titled "cute" and found that it contained 12 non-pornographic images,

each different from those found in talentedtongue19's "cute" album. However, SA Ruiz found at least two images within tongueboy's album that depicted what appeared to be the same young male child that SA Ruiz found in talentedtongue19's image album.

23. On or about August 7, 2015, SA Ruiz conducted a search on Google.com for Internet content matching "talentedtongue14". The search resulted in the identification of another Website A user account registered as "talentedtongue14." SA Ruiz accessed the profile page and found that the account had been shut down by Website A administrators. The profile page for talentedtongue14 stated "Account locked out for child abuse/exploitation."

24. On or about November 17, 2015, SA Ruiz sent an email to HSI Intelligence Research Specialist (IRS) Lauren Morris inquiring if IRS Morris had any information or received leads on Website A users talentedtongue19, talentedtongue14, and/or tongueboy. On or about November 18, 2015, IRS Morris informed SA Ruiz that IRS Morris did not have any prior leads on the requested users; however, IRS Morris had conducted a search within Google.com and found the email address talentedtongue14@hotmail.com. IRS Morris subsequently conducted a search of that email address within the social networking website Facebook.com. IRS Morris found a single user profile registered to a Randy GUM in Rochester, Pennsylvania (www.facebook.com/randy.gum.1). IRS Morris informed SA Ruiz that GUM's Facebook profile contained some of the same photos, depicting a young male child, that are contained in the "cute" albums uploaded to the Website A accounts talentedtongue19 and tongueboy.

25. On or about November 18, 2015, SA Ruiz accessed GUM's Facebook.com profile at www.facebook.com/randy.gum.1. SA Ruiz found that the profile was publicly accessible and that photos, postings, and relationships information posted to the profile were all

publicly accessible and not set to private. SA Ruiz reviewed the photos uploaded to GUM's Facebook profile and found approximately 25 pictures depicting the same young male child contained in the image albums found on the talentedtongue19 and tongueboy Website A accounts. One of the photos found on GUM's Facebook.com profile was uploaded on or about January 30, 2013. The photo depicts the young male child and GUM together. The photo appears to have been uploaded with the comment "Lil bro." SA Ruiz reviewed the comments posted to the photo and found that on January 30, 2013, GUM posted the comment to the photo stating "I got a new #. 7245062757 hmu". This is the same phone number that Yahoo! reported as being registered to the email account talentedtongue19@yahoo.com. Additionally, on June 9, 2013, a photo was uploaded to the GUM Facebook account depicting the young male child holding up two wrestling action figures. The photo was uploaded with the caption "Like my son right there." SA Ruiz found the same photo uploaded to the "cute" image album on the talentedtongue19 Website A profile.

26. In December 2015, your Affiant received the aforementioned investigative lead from SA Ruiz. During your Affiant's review of this information, your Affiant noted several different email accounts associated with Randy GUM, including talentedtongue19@yahoo.com, talentedtongue14@yahoo.com, talentedtongue14@hotmail.com, and randygum94@gmail.com. Additionally, your Affiant noted the following two Facebook accounts for Randy GUM: randy.gum.1 (Facebook User ID 100000421615731) and randy.gum.9 (Facebook User ID 100009052827992). Your Affiant subsequently searched a law enforcement database for the names "Randolph GUM" and "Randy GUM," resulting in an arrest photo for a Randolph Guy GUM, DOB: 02/23/1994.

Your Affiant noted that the arrest photo of GUM depicts the same individual with the Facebook accounts randy.gum.1 and randy.gum.9.

27. While reviewing the information obtained from Yahoo! pursuant to the federal search warrant for the talentedtongue19@yahoo.com account, your Affiant reviewed an email string between talentedtongue19@yahoo.com and damnhegotstupidass@yahoo.com from July 2015. Within this email conversation, talentedtongue19@yahoo.com included an attachment named VID-20140322-WA0007.mp4. Your Affiant reviewed this attachment, which contained a video that is approximately one minute and forty-two seconds in length (1:42) and shows an adult male penis penetrating the anus of a prepubescent male child. Within this same email string, talentedtongue19@yahoo.com writes, "Send me more of what you got" followed by this link to Dropbox:

https://www.dropbox.com/sh/mnrec2g1rwe7lvh/AAD3lC0HtlpcRJw28oc4686oa?dl=0

Your Affiant reviewed this Dropbox link and found that it included approximately 2,479 images, the vast majority of which were child pornography and child erotica depicting prepubescent and pubescent male children.

28. On January 26, 2016, your Affiant submitted a preservation request to Facebook for the accounts randy.gum.1 (Facebook User ID 100000421615731) and randy.gum.9 (Facebook User ID 100009052827992). On or about February 10, 2016, your Affiant served DHS summonses upon Facebook for subscriber information pertaining to these two Facebook accounts.

29. On or about February 11, 2016, Facebook responded with subscriber information for each of these accounts. For Facebook account randy.gum.1 (Facebook User ID 100000421615731), the name provided was "Randy Gum" with the registered email addresses

randy.gum.1@facebook.com, rgum94@hotmail.com, and talentedtongue14@hotmail.com. For Facebook account randy.gum.9 (Facebook User ID 100009052827992), the name provided was "Randy Gum" with the registered email address rgum94@hotmail.com.

30. On February 29, 2016, your Affiant executed a search and seizure warrant upon Dropbox for the account user talentedtongue14@yahoo.com for evidence related to the violation of federal child exploitation laws.

31. On March 25, 2016, your Affiant received the Dropbox response to the aforementioned search warrant, including one 8-gigabyte thumb drive containing files from the talentedtongue14@yahoo.com Dropbox account. Your Affiant later reviewed these files and found hundreds of images and videos depicting the sexual exploitation of minors, to include infants, toddlers, and prepubescent children. Your Affiant also noted that the Dropbox account talentedtongue14@yahoo.com was registered to the name "Randy GUM."

32. On April 7, 2016, HSI Pittsburgh Special Agent (SA) David Coleman conducted a review of the GUM Dropbox Search Warrant return. The review of this search warrant return was conducted using included using NetClean Analyze DI version number 15.2.3. SA Coleman classified approximately 8,660 photographs and videos from the GUM Dropbox Search Warrant return. The 8,660 photographs and videos contained duplicates. SA Coleman identified 5,486 visually unique photographs and 90 visually unique videos. Of the visually unique photos and videos identified, most depicted child exploitation material (CEM) or child abuse material (CAM).

33. Further review of the Camera Uploads folder in GUM's Dropbox uncovered multiple images and videos of child abuse material that appears to be produced by GUM. Specifically, GUM is clearly visible in two (2) of the videos performing sex acts on a pre-

pubescent male child. Two (2) of the seven (7) videos show a prepubescent boy performing oral sex on an adult male. Two (2) of the seven (7) videos showed the same pre-pubescent boy being anally penetrated by an adult male. One (1) of the seven (7) videos showed the same pre-pubescent boy and an adult male (identified as GUM) mutually masturbating each other and GUM inserting GUM's finger into the anus of the minor male child. One (1) of the seven (7) videos showed the same pre-pubescent boy having his naked buttocks fondled by an adult male. One (1) of the seven (7) videos showed the same pre-pubescent boy having his anus licked by an adult male (identified as GUM). The videos were recorded during the timeframe of January, 2014 to April, 2014.

34. Based upon review and investigation by your Affiant, it has been determined that the pre-pubescent male victim is known to this investigation and this victim was previously physically assaulted by GUM. GUM is currently awaiting sentencing for charges related to the assault of the victim. The male child is also the same male child depicted with GUM in photographs on GUM's Facebook.com profiles described in paragraph 25 above.

Facebook

35. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

36. Facebook asks users to provide basic contact information to Facebook, either during the registration process or thereafter. This information may include the user's full name,

birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

37. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

38. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "Mini-Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

39. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. A particular user's profile page also includes a "Wall," which is a space where the user and his or

her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

40. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, a user's "Photoprint" includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

41. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

42. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

43. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

44. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

45. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

46. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

47. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

48. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments

associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

49. Therefore, the computers of Facebook are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and account application.

CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN RECEIVING CHILD PORNOGRAPHY AND WHO HAVE A SEXUAL INTEREST IN CHILDREN AND IMAGES OF CHILDREN

50. Based on your Affiant's previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom your Affiant has had discussions, your Affiant has learned that individuals who view and receive multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or mobile device. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names,

addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Those that receive and possess and collect child pornography maintain their collection and material even if they move physical, geographic locations. A collector and user of child pornography who maintains the images and videos in a digital or electronic format, such as on a computer, discs, external hard drive, thumb drives, mobile devices, etc., will take the materials to a new location in the event of a physical move.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

51. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

52. Based on the forgoing, I request that the Court issue the proposed search warrant.

53. This Court has jurisdiction has jurisdiction to issue the proposed order because it is "a court of competent jurisdiction," as defined in 18 U.S.C. § 2711 and 18 U.S.C. § 2703(d). Specifically, this Court is a district court of the United States that has jurisdiction over the offenses being investigated. See 18 U.S.C. § 2711(3)(A)(i).

54. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

Molly Rock
Special Agent
ICE-HSI

Subscribed and sworn to before me on April 12, 2016

ROBERT C. MITCHELL
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Facebook user IDs **100000421615731 (randy.gum.1)** and **100009052827992 (randy.gum.9)** that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Palo Alto, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

(a) All contact information, including: full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All Photos or videos, in their original file format, including any and all EXIF data, and including all photos uploaded by that user ID and all photos uploaded by any user that have that user tagged in them;

(c) All Neoprints, including profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(d) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(i) All information about the Facebook pages that the account is or was a "fan" of;

(j) All past and present lists of friends created by the account;

(k) All records of Facebook searches performed by the account;

(l) All information about the user's access and use of Facebook Marketplace;

(m) The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);

(n) All information concerning page views of 3rd party websites that contain the "like" button of other Facebook social elements;

(o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252(a)(2), and 2252(a)(4)(B) involving Randolph "Randy" GUM since **11/02/2009**, including, for each user ID identified on Attachment A, information pertaining to the following matters:

(a) Messages, correspondence, documents and records pertaining to the production, receipt, distribution, and/or possession of material depicting the sexual exploitation of minors, as well as information indicating the location of the account user and the identity of the account user.

(b) Records relating to who created, used, or communicated with the user IDs, including records about their identities and whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Facebook, and my official title is _____. I am a custodian of records for Facebook. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Facebook, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Facebook; and

c. such records were made by Facebook as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature